(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 44 39 266 A 1**

(51) Int. Cl.[6]:
G 06 K 19/10
G 06 K 19/073
G 06 F 7/08

(21) Aktenzeichen: P 44 39 266.4
(22) Anmeldetag: 3. 11. 94
(43) Offenlegungstag: 11. 4. 96

DE 44 39 266 A 1

(30) Innere Priorität: (32) (33) (31)
30.09.94 DE 44 35 137.2

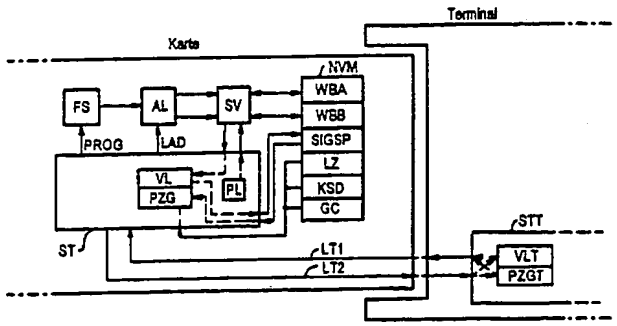
(71) Anmelder:
Siemens AG, 80333 München, DE

(72) Erfinder:
Schrenk, Hartmut, Dr., 85540 Haar, DE

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Datenübertragungssystem mit einem Terminal und einer tragbaren Datenträgeranordnung und Verfahren zum Wiederaufladen der tragbaren Datenträgeranordnung mittels des Terminals

(57) Bei einem Datenübertragungssystem, das mit zumindest einem Terminal und zumindest einer tragbaren Datenträgeranordnung, beispielsweise einer Chipkarte, gebildet ist, ist der einen Geldwert repräsentierende Bereich des nichtflüchtigen Speichers (NVM) der Karte in zwei Wertbereiche (WBA, WBB) unterteilt, von denen jeweils nur einer (WBA bzw. WBB) nicht-flüchtig aktivierbar ist und der andere (WBB bzw. WBA) nur vorläufig aktiviert werden kann. Beim Wiederaufladen der Karte wird der neue Zählerstand in den zunächst nur vorläufig aktivierten Wertbereich (WBB) geschrieben und erst nach Überprüfung des korrekten Schreibens dieser Wertbereich (WBB) nicht-flüchtig aktivierbar geschaltet.



DE 44 39 266 A 1

Beschreibung

Die Erfindung betrifft ein Datenübertragungssystem mit zumindest einem Terminal und mit zumindest einer tragbaren Datenträgeranordnung, die mit einem nichtflüchtigen Halbleiterspeicher versehen ist, der zumindest einen ersten als Zähler fungierenden, einen abbuchbaren Geldwert repräsentierenden Wertbereich aufweist sowie ein Verfahren zum Wiederaufladen des Wertbereichs der tragbaren Datenträgeranordnung.

Eine solche tragbare Datenträgeranordnung ist beispielsweise eine heute gebräuchliche Chipkarte, die beispielsweise als Telefonkarte benutzt wird. In diesem Fall ist das stationäre Terminal ein kartentauglicher Telefonapparat. Solche als einfache Speicherkarten ausgeführten Chipkarten enthalten einen nicht-flüchtigen Halbleiterspeicher, beispielsweise ein EEPROM, das im wesentlichen als Zähler für die voraus bezahlten und abzubuchenden Telefoneinheiten fungiert. Das EEPROM kann dabei beispielsweise gemäß der EP-B 0321 727 bzw. US-A 5,001,332 beschaltet sein, so daß es als mehrstufiger, Abacus-ähnlicher Zähler arbeitet. Der Wert der Karte und damit der Zählumfang des Zählers wird durch Beschreiben und damit Blockieren der Bereiche des Zählers, die nicht mehr erlaubt sein sollen, festgelegt. Vor dieser Festlegung hat der Zähler immer den maximalen Zählumfang. Heute übliche Telefonkarten sind nur einmal zu gebrauchen und werden nach dem Gebrauch weggeworfen. Es ist aber auch der Gebrauch solcher Chipkarten als elektronische Geldbörse im Gespräch. Für diesen Zweck verwendbare Chipkarten sind nur sinnvoll, wenn sie wiederaufladbar sind, wenn also der Zählerstand wieder erhöht werden kann, nachdem ein gewisser Betrag abgebucht worden ist. Diese Erhöhung des Zählerstands findet an speziellen Ladeterminals statt, an denen der Benutzer entweder durch Bareinzahlung, mittels Kreditkarte oder durch Angabe einer Kontonummer einen gewünschten Betrag auf seine Karte aufbuchen kann. Beim Wiederaufladen des Zählers einer Chipkarte kann es aufgrund des Aufbaus von EEPROMs erforderlich sein, zunächst einen größeren Zählbereich oder den gesamten Zähler zu löschen, das heißt es wird vorübergehend ein zu hoher Zählumfang eingestellt. Erst danach kann der neue Zählerstand durch erneute Begrenzung des Zählumfangs durch Programmiervorgänge eingestellt werden.

Wenn ein Benutzer in der Zeit zwischen dem Löschen des Zählers und dem erneuten Programmieren die Karte aus dem Terminal zieht, hätte er einen zu hohen Betrag aufgebucht bekommen, wodurch eine mißbräuchliche Manipulation ermöglicht wird. Außerdem ist es denkbar, daß ein Benutzer den Datenverkehr zwischen Terminal und Karte manipuliert, so daß auf diese Weise ein zu hoher Betrag aufgebucht werden kann.

Die Manipulation der Daten auf den Übertragungsweg könnte durch eine sogenannte elektronische Unterschrift verhindert werden. Die zu übermittelnden Daten können außerdem mittels eines geheimen Schlüssels verschlüsselt werden und können nur mit einem bestimmten, eindeutig dem Absender der Daten zuzuordnenden Schlüssel entschlüsselt werden, wodurch der Absender eindeutig identifizierbar wird und die Daten nicht manipuliert werden können, da der Verschlüsselungsschlüssel geheim ist. Eine solche Verschlüsselung und Entschlüsselung erfordert jedoch ein aufwendiges und sehr schnelles Rechenwerk, das nur mit teuren Mikroprozessoren möglich ist, wie sie beispielsweise in bereits bekannten Kryptokarten benutzt werden.

Aufgabe der Erfindung ist es somit, ein gattungsgemäßes Datenübertragungssystem und ein Verfahren anzugeben, bei dem auf einfache Weise eine manipulationssichere Wiederaufladung des Zählers der tragbaren Datenträgeranordnung möglich ist.

Die Aufgabe wird dadurch gelöst, daß in dem nichtflüchtigen Halbleiterspeicher ein zweiter Wertbereich vorhanden ist, wobei nur jeweils einer der beiden Wertbereiche nicht-flüchtig aktivierbar ist und der jeweils andere Wertbereich nur vorläufig aktiviert werden kann.

Nicht-flüchtig aktivierbar bedeutet hierbei, daß die Information, welcher der beiden Wertbereiche zuletzt als Wertbereich, von dem abgebucht werden konnte, definiert war, auch nach Abschalten der Betriebsspannung oder bei Unterbrechung des Ladevorgangs erhalten bleibt. Das bedeutet, daß ein nur vorläufig aktivierter Wertbereich nach Abschalten der Betriebsspannung bzw. Unterbrechung des Ladevorgangs und Wiedereinschalten der Betriebsspannung bzw. Neubeginn eines Ladevorgangs wieder deaktiviert ist und nochmals vorläufig aktiviert werden muß. Erst nach erfolgreichem und korrektem Wiederaufladen der Chipkarte, d. h. erst nach korrektem Begrenzen des Zählumfangs des nur vorläufig aktivierten Wertbereichs entsprechend der Summe aus dem Restwert und einem ins Terminal eingegebenen auf zubuchenden Wert wird der nur vorläufig aktivierte Wertbereich nicht-flüchtig aktivierbar geschaltet, wodurch der zuvor nicht-flüchtig aktivierte Wertbereich deaktiviert wird und für einen neuen Ladevorgang zunächst nur vorläufig aktiviert werden kann.

Wenn also ein Betrüger versuchen würde, beim Ladevorgang des nur vorläufig aktivierten Wertbereichs nach dem Löschen des Zählers und vor dem erneuten Begrenzen seines Zählumfangs entsprechend dem einzugebenden Wert die Karte aus dem Terminal zu entfernen, so würde bei der nächsten Benutzung, also beim nächsten Anlegen der Betriebsspannung weiterhin der nicht-flüchtig aktivierbare Wertbereich aktiviert werden und der zuvor nur vorläufig aktivierte Wertbereich wäre deaktiviert.

In vorteilhafter Weiterbildung der Erfindung sind die Wertbereiche des nicht-flüchtigen Speichers gemäß Anspruch 2 über eine Auswahl-Logikschaltung mit einem nicht-flüchtigen Flag-Speicher, dessen Zustand den nicht-flüchtig aktivierten Wertbereich bestimmt, verbunden. Beim Abschalten der Betriebsspannung bleibt der Zustand des nicht-flüchtigen Flag-Speichers erhalten, wobei ein bestimmter Zustand immer demselben Wertbereich zugeordnet ist.

Zum vorläufigen Aktivieren des jeweils anderen Wertbereichs ist in erfindungsgemäßer Weise die Auswahl-Logikschaltung mit einem Ladesteuersignal beaufschlagbar. Dieses Ladesteuersignal hat in seinem neutralen Zustand, d. h. dem Zustand nach dem Anlegen der Betriebsspannung beispielsweise einen logischen "0"-Pegel und wird zum vorläufigen Aktivieren des neu zu ladenden Wertbereich entsprechend auf einen "1"-Pegel umgeschaltet.

Das oder die Ausgangssignal(e) steuern eine Schaltvorrichtung an, die die Wertbereiche mit einer Programmier-Logikschaltung und einer Verifizier-Logikschaltung verbindet. Ein Wertbereich wird also dadurch aktiviert, daß er mit der Programmier-Logikschaltung und der Verifizier-Logikschaltung verbunden wird.

Die tragbare Datenträgeranordnung bzw. Chipkarte des erfindungsgemäßen Datenübertragungssystems und die vorteilhaften Weiterbildungen dieses Systems

werden durch ein Verfahren gemäß dem Anspruch 5 wieder aufgeladen. Vorteilhafte Weiterbildungen des Verfahrens sind in den abhängigen Ansprüchen angegeben.

Die Erfindung wird nachfolgend mit Hilfe eines Ausführungsbeispiels anhand einer Figur näher erläutert. Dabei zeigt die Figur in schematischer Form ein Ladeterminal sowie eine in dieses eingeführte tragbare Datenträgeranordnung. Die erfindungswesentlichen Schaltungsanordnungen der beiden Teile des Datenübertragungssystems sind in Form eines Blockschaltbilds dargestellt.

Eine tragbare Datenträgeranordnung, im folgenden Karte genannt, wobei auch andere Ausführungsarten, beispielsweise als Schlüssel, denkbar sind, ist in der Figur in ein Ladeterminal eines Datenübertragungssystems eingeführt. Die Karte beinhaltet einen nichtflüchtigen Speicher NVM, der in vorteilhafter Weise durch ein EEPROM realisiert sein kann. Dieser Speicher NVM ist dabei in mehrere Bereiche unterteilt, wovon zwei als Wertbereiche WBA, WBB fungieren. Diese Wertbereiche WBA, WBB sind in vorteilhafter Weise als mehrstufige Zähler ausgeführt und beispielsweise gemäß der EP-B 0321 727 bzw. US-A 5,001,332 beschaltet. Solche Zähler sind Abwärtszähler, wenn sie im gelöschten oder aufgeladenen Zustand den logischen Zustand "1" und damit einen maximalen, durch die Anzahl der Zählstufen und Bits pro Stufe bestimmten Zählumfang haben. Durch Beschreiben einer geeigneten Anzahl oberer Stufen bzw. einiger Bits der untersten dieser oberen Stufen läßt sich der Zählumfang begrenzen und ab diesem Sollwert bis zum Endwert "0" herunterzählen.

Die Wertbereiche WBA, WBB sind über eine Schaltvorrichtung SV mit einer Programmier-Logikschaltung PL und einer Verifizier-Logikschaltung VL verbunden. Die Programmier-Logikschaltung PL und die Verifizier-Logikschaltung VL sind dabei Bestandteile einer Steuereinrichtung ST. Innerhalb der Steuereinrichtung ST sind die Verbindungslinien der Schaltungsteile strichliert dargestellt, womit angedeutet werden soll, daß die jeweilige Verbindungslinie zur Steuereinrichtung ST innerhalb der Steuereinrichtung ST auch mit anderen, nicht dargestellten Teilen der Steuereinrichtung ST verbunden sein kann.

Die Programmier-Logikschaltung PL dient zum Programmieren bzw. Beschreiben der Wertbereiche WBA, WBB und die Verifizier-Logikschaltung VL zum Verifizieren bzw. Überprüfen der beschriebenen Bereiche, ob richtig beschrieben wurde. In vorteilhafter Weise dient die Verifizier-Logikschaltung VL auch zur Erzeugung einer elektronischen Signatur eines Wertzustandes.

Die Schaltvorrichtung SV wird von einer Auswahl-Logikschaltung AL derart angesteuert, daß jeweils nur einer der Wertbereiche WBA, WBB mit der Programmier-Logikschaltung PL und Verifizier-Logikschaltung VL verbunden und dadurch aktiviert ist. Die Auswahl-Logikschaltung AL wird ihrerseits von einem Flag-Speicher FS und über ein Ladesteuersignal LAD von der Steuereinrichtung ST angesteuert. Die Auswahl-Logikschaltung AL kann beispielsweise mit einem EXOR-Gatter mit einem nicht-invertierenden und einem invertierenden Ausgang gebildet sein. Der Flag-Speicher FS ist ein nicht-flüchtiger Speicher und wird über ein Signal PROG von der Steuereinrichtung ST angesteuert. Der Flag-Speicher FS kann zwei Zustände einnehmen, wobei jeder dieser Zustände einem der Wertbereiche WBA, WBB zugeordnet ist. Da der Zustand des Flag-Speichers FS nicht-flüchtig gespeichert ist, wird bei Anlegen der Betriebsspannung an die Karte, d. h. beispielsweise durch Einführen der Karte in das Ladeterminal, der dem jeweils gespeicherten Zustand entsprechende Wertbereich WBA bzw. WBB aktiviert. Das Ladesteuersignal LAD nimmt hierzu beim Anlegen der Betriebsspannung einen definierten Zustand ein. Erst nach Ändern des Zustands des Ladesteuersignals LAD wird mittels der Schaltvorrichtung SV, die von der Auswahl-Logikschaltung AL entsprechend angesteuert wird, der jeweils andere Wertbereich WBB bzw. WBA vorläufig aktiviert und der zuvor aktivierte Wertbereich WBA bzw. WBB deaktiviert. Vorläufig deshalb, weil der Zustand des Ladesteuersignals flüchtig ist und bei Abschalten der Betriebsspannung, was z. B. durch Entfernen der Karte aus dem Ladeterminal erfolgt, wieder seinen definierten inaktiven Zustand einnimmt, so daß nach jedem Abschalten der Betriebsspannung oder erfindungsgemäß nach jedem Unterbrechen eines Ladevorgangs wieder der durch den Flag-Speicher FS definierte Wertbereich aktivierbar bzw. aktiviert ist.

Durch ein Signal PROG von der Steuereinrichtung ST zum Flag-Speicher FS kann eine Änderung des Zustands des Flagspeichers und damit der Austausch des aktivierten bzw. aktivierbaren Wertbereichs nichtflüchtig durchgeführt werden.

Der nicht-flüchtige Speicher NVM enthält als weitere Bereiche einen Signaturspeicher SIGSP, der später erläutert wird, einen Ladezähler LZ, mit dem die Ladevorgänge gezählt werden können, einen Bereich KSD, in dem kartenspezifizische Daten abgespeichert sind und einen Bereich GC, in dem ein geheimer Code gespeichert ist.

In der Steuereinrichtung ST ist außerdem ein Pseudo-Zufalls-Generator PZG enthalten, der in Wirkverbindung mit der Verifizier-Logikschaltung VL steht und außerdem mit dem Signaturspeicher SIGSP, dem Ladezähler LZ, dem Bereich KSD und dem Geheimcodebereich GC des nicht-flüchtigen Speichers NVM verbunden ist. Dieser Pseudo-Zufallsgenerator PZG ist in vorteilhafter Weise gemäß der EP-A 0 616 429 aufgebaut.

Auch im Ladeterminal ist eine Steuereinrichtung STT enthalten, die ebenfalls eine Verifizier-Logikschaltung VLT und einen Pseudo-Zufallsgenerator PZGT enthält, wobei die beiden Pseudo-Zufallsgeneratoren PZG und PZGT identisch sein müssen, wenn die Karte und das Terminal echt sind. Die Steuereinrichtung ST der Karte und die Steuereinrichtung STT des Terminals stehen über Leitungen LT1, LT2 miteinander in Verbindung, um Daten austauschen zu können.

Zu Beginn eines Ladevorgangs liest das Terminal die kartenspezifischen Daten, den aktuellen Stand des aktivierten und damit abbuchbaren Wertbereichs WBA bzw. WBB sowie den Stand des Ladezählers LZ und des Signaturspeichers SIGSP. Aus den kartenspezifischen Daten kann ein echtes Terminal beispielsweise mittels einer Tabelle den Geheimcode der Karte ermitteln. Diese Daten sowie eine weitere Zufallszahl, die sogenannte Challenge, werden im Terminal in den Pseudo-Zufallsgenerator PZGT eingegeben, der eine Response berechnet. Sowohl die Challenge als auch die Response werden daraufhin an die Karte übermittelt. Dort wird ebenfalls anhand der Daten eine Response berechnet und mit der vom Terminal übermittelten Response mittels eines Komparators, der ebenfalls in der Steuereinrichtung ST enthalten ist, verglichen. Bei Übereinstimmung hat sich das Terminal als echt ausgewiesen, da es zum einen in der Lage war, den richtigen Geheimcode zu ermitteln, und außerdem den richtigen Pseudo-Zu-

fallsgenerator PZGT hat.

Der Pseudo-Zufallsgenerator PZG bzw. PZGT dient auch dazu, eine elektronische Signatur des Inhalts der Wertbereiche WBA, WBB, also derer Zählerstände zu erzeugen. Da das Ausgangssignal des Pseudo-Zufallsgenerators von dem Geheimcode der Karte abhängt und nur mit diesem geheimen Code nachgerechnet werden kann, muß bei Übereinstimmung von Ausgangssignalen des Pseudo-Zufallsgenerators PZG bzw. PZGT derselbe geheime Code verwendet worden sein. Somit ist das Ausgangssignal eines Pseudo-Zufallsgenerators eindeutig einer bestimmten Karte zuordenbar, was als Signatur der Karte unter dem Zählerstand bezeichnet wird.

Damit durch eine Analyse mehrerer Berechnungsvorgänge der Aufbau des Pseudo-Zufallsgenerators und die eingegebenen Daten nicht ermittelt werden können, sind ein oder mehrere der eingegebenen Daten veränderbar und verändern sich auch mit jedem Berechnungsvorgang. Eines dieser Daten ist der Stand des Ladezählers LZ, der mit jedem neuen Ladevorgang und damit mit jedem neuen Buchungsvorgang um 1 erhöht wird bzw. rückgesetzt wird, wenn der Zählumfang erschöpft ist.

Ein anderes Datum ist der Inhalt des Signaturspeichers SIGSP. In diesen wird jeweils das Ergebnis einer vorherigen Rechnung des Pseudo-Zufallsgenerators eingeschrieben, die ja eine Signatur des vorherigen Zählerstandes ist. Damit ist sichergestellt, daß sich das Ausgangssignals des Pseudo-Zufallsgenerators PZG nur mit verschwindender Wahrscheinlichkeit wiederholt und somit nicht analysiert werden kann.

In den Signaturspeicher SIGSP kann in einer Variante der Erfindung als Signatur des Ladevorgangs über das Ladeterminal bei jedem Ladevorgang ein neuer Wert direkt eingeschrieben werden.

Ein erfindungsgemäßer Ladevorgang läuft in einfachster Weise derart ab, daß nach Einführen der Karte in das Ladeterminal und damit nach Anlegen einer Betriebsspannung der durch den Zustand des Flag-Speichers FS definierte Wertbereich WBA oder WBB aktiviert ist und vom Terminal ausgelesen wird. Durch Ändern des Zustands des Ladesteuersignals LAD wird der andere Wertbereich WBB oder WBA vorläufig aktiviert und der zuvor aktivierte vorläufig deaktiviert. Dann wird der nunmehr aktivierte Wertbereich WBB oder WBA gelöscht, wobei dessen Zähler einen zu großen Zählumfang annimmt. Daraufhin wird im Terminal aus dessen alten Zählerstand und dem vom Benutzer ins Terminal eingegebenen auf zubuchenden Betrag ein neuer Zählerstand ermittelt und an die Karte übertragen. Würde der Benutzer vorher die Karte aus dem Terminal entfernen, hätte er einen zu hohen Betrag aufgebucht bekommen, wenn die Programmierung des Wertbereichs bereits endgültig und nicht-flüchtig erfolgt wäre. Durch erneutes Einführen der Karte in das Terminal wird aber in erfindungsgemäßer Weise wieder der vorherige Wertbereich WBA bzw. WBB mit dem alten Zählerstand aktiviert, da der Zustand des Flag-Speichers FS noch nicht geändert worden war. Erst wenn der neue Zählerstand in den vorläufig aktivierten Wertbereich WBB bzw. WBA einprogrammiert wurde, wird der Zustand des Flag-Speicher FS durch ein Signal PROG von der Steuereinrichtung ST geändert, wodurch der neue Wertbereich nicht-flüchtig aktivierbar ist und bei jedem neuen Anlegen der Betriebsspannung, also bei jedem Einführen der Karte in ein Terminal aktiviert wird, beispielsweise um Geld abzubuchen.

Um eine Manipulation des neuen Zählerstandes bei der Übertragung vom Terminal zur Karte zu verhindern, wird in erfindungsgemäßer Weiterbildung des Verfahrens nach dem Übertragen des neuen Zählerstandes zur Karte dort gemäß dem oben beschriebenen Verfahren der Zählerstand signiert. Die Signatur wird anschließend zum Terminal übertragen und dort mit einer ebenfalls ermittelten Signatur verglichen. Bei Übereinstimmung ist sichergestellt, daß der richtige Zählerstand zur Karte übertragen wurde. Bei Nicht-Übereinstimmung wird der Ladevorgang abgebrochen, wodurch der falsche Zählerstand keinen Einfluß auf spätere Abbuchvorgänge hat, da der Zustand des Flag-Speichers FS noch nicht geändert wurde. Dieser wird erst nach Erkennen der Übereinstimmung der Signaturen und Übermitteln eines entsprechenden Signals vom Terminal an die Karte geändert.

In Weiterbildung des erfindungsgemäßen Verfahrens muß sich das Terminal gegenüber der Karte authentifizieren, bevor ein Ladevorgang gestartet werden kann. Dadurch ist sichergestellt, daß kein falsches Ladegerät zum Aufbuchen einer Karte benutzt werden kann. Für diese Authentifizierung werden aus den vom Terminal aus der Karte gelesenen Daten und einer Challenge eine Response berechnet, die zusammen mit der Challenge an die Karte übermittelt und dort mit einem ebenfalls mittels der Challenge und den Kartendaten berechneten Response verglichen wird. Nur bei Übereinstimmung der Responses können das Ladesteuersignal LAD und auch das Programmiersignal PROG erzeugt und damit ein Ladevorgang begonnen werden. Zu diesem Zweck sind in der tragbaren Datenträgeranordnung Freigabevorrichtungen FGV1, FGV2 vorgesehen, die von der Steuereinrichtung ST geeignet angesteuert werden. Ein solcher Ladevorgang wird dabei beispielsweise durch Erhöhen des Standes des Ladezählers LZ oder durch einen Dummy-Programmierimpuls gestartet. Ein Dummy-Programmierimpuls ist dabei ein Programmierimpuls auf eine nicht-gültige Adresse des nicht-flüchtigen Speichers NVM, der von der Steuereinrichtung ST der Karte als Steuerbefehl erkannt wird.

Auch nach dem Start eines Ladevorganges, nachdem das Terminal seine Berechtigung nachgewiesen hat und das Ladesignal LAD erzeugt worden ist, könnte es einem Betrüger gelingen, Einfluß auf den Wert des Zählerstandes zu nehmen und das Programmiersignal PROG zur nicht-flüchtigen Aktivierung des Zählerstandes unabhängig vom Terminal auszulösen. In einer Weiterbildung des erfindungsgemäßen Verfahrens muß vor Erzeugung des Programmiersignals PROG das Terminal noch einmal seine Berechtigung nachweisen, das heißt, es muß sich noch einmal authentifizieren. Die Erzeugung der Responses entspricht dabei der bei der ersten Berechtigungsprüfung zum Start eines Ladevorgangs.

Um eine Wiederholung von Responses zu verhindern, die von der Datenträgeranordnung im Rahmen einer Signaturberechnung ausgegeben werden und zur Erzeugung des Programmiersignals PROG ausgenutzt werden könnten, wird zur Erzeugung einer Response in erfindungsgemäßer Weise ein sich bei jeder Responseberechnung änderndes Datum verwendet. Dieses Datum wird durch einen Responsezähler RZ geliefert, der vor jeder Responseberechnung nicht-flüchtig geändert wird und dessen Zählerstand die Responseberechnung beeinflußt. Der Responsezähler RZ ist in vorteilhafter Weise als Bereich des nicht-flüchtigen Speichers realisiert.

Durch das erfindungsgemäße Datenübertragungssy-

stem und das erfindungsgemäße Verfahren wird eine sichere Wiederaufladung einer tragbaren Datenträgereinrichtung, beispielsweise einer Chipkarte erreicht.

Patentansprüche

1. Datenübertragungssystem mit zumindest einem Terminal und mit zumindest einer tragbaren Datenträgeranordnung, die mit einem nicht-flüchtigen Halbleiterspeicher (NVM) versehen ist, der zumindest einen ersten als Zähler fungierenden, einen abbuchbaren Geldwert repräsentierenden Wertbereich (WBA) aufweist, **dadurch gekennzeichnet,** daß der nicht-flüchtige Halbleiterspeicher (NVM) einen zweiten als Zähler fungierenden Wertbereich (WBB) aufweist, wobei nur jeweils einer der beiden Wertbereiche (WBA bzw. WBB) nicht-flüchtig aktivierbar ist und der jeweils andere Wertbereich (WBB bzw. WBA) nur vorläufig aktiviert werden kann.

2. Datenübertragungssystem nach Anspruch 1, dadurch gekennzeichnet, daß die Wertbereiche (WBA, WBB) des nicht-flüchtigen Speichers (NVM) über eine Auswahl-Logikschaltung (AL) mit einem nicht-flüchtigen Flagspeicher (FS), dessen Zustand den nicht-flüchtig aktivierten Wertbereich (WBA bzw. WBB) bestimmt, verbunden sind.

3. Datenübertragungssystem nach Anspruch 2, dadurch gekennzeichnet, daß die Auswahl-Logikschaltung (AL) mit einem Ladesteuersignal (LAD) beaufschlagbar ist, das die vorläufige Aktivierung des nicht nicht-flüchtig aktivierten Wertbereichs (WBB bzw. WBA) bewirkt und den nicht-flüchtig aktivierten Wertbereich (WBA bzw. WBB) vorläufig deaktiviert.

4. Datenübertragungssystem nach Anspruch 2 oder 3, dadurch gekennzeichnet, daß zwischen der Auswahl-Logikschaltung (AL) und dem nicht-flüchtigen Speicher (NVM) eine Schaltvorrichtung (SV) vorgesehen ist, die in Abhängigkeit von dem oder den Ausgangssignal(en) der Auswahl-Logikschaltung (AL) eine Programmier-Logikschaltung (PL) und eine Verifizier-Logikschaltung (VL) mit dem jeweils aktiven Wertbereich (WBA bzw. WBB) verbindet.

5. Datenübertragungssystem nach Anspruch 3, dadurch gekennzeichnet, daß in der Datenträgeranordnung eine erste Freigabevorrichtung (FGV1) vorgesehen ist, die die Erzeugung eines Ladesignals (LAD) erst nach einer positiven Authentifizierung des Terminals zuläßt.

6. Datenübertragungssystem nach einem der Ansprüche 2 bis 5, dadurch gekennzeichnet, daß der nicht-flüchtige Flagspeicher (FS) mit einem Programmiersignal (PROG) beaufschlagbar ist, das die Umwandlung des vorläufig aktivierten Wertbereichs (WBB bzw. WBA) in den nicht-flüchtig aktivierbaren Wertbereich (WBA bzw. WBB) veranlaßt.

7. Datenübertragungssystem nach Anspruch 6, dadurch gekennzeichnet, daß in der Datenträgeranordnung eine zweite Freigabevorrichtung (FGV2) vorgesehen ist, die die Erzeugung des Programmersignals (PROG) erst nach einer positiven Authentifizierung des Terminals zuläßt.

8. Datenübertragungssystem nach Anspruch 5 oder 7, dadurch gekennzeichnet, daß der nicht-flüchtige Halbleiterspeicher (NVM) einen als nicht-flüchtige Zählvorrichtung fungierenden Freigabebereich (FGB) aufweist, in dem jeder Versuch zur Erlangung der Freigabe nicht-flüchtig registrierbar ist und der aufeinanderfolgende Freigabeprozeduren unterscheidbar macht.

9. Verfahren zum Wiederaufladen einer einen Geldwert repräsentierenden tragbaren Datenträgeranordnung mittels eines Terminals eines Datenübertragungssystem gemäß einem der Ansprüche 1 bis 8 mit den Schritten:

a) Lesen des alten Zählerstandes des nicht-flüchtig aktivierten Wertbereichs (WBA bzw. WBB) aus der tragbaren Datenträgeranordnung mittels des Terminals

b) Berechnen eines neuen Zählerstandes aus dem alten Zählerstand und in das Terminal eingegebenen aufzubuchenden Daten im Terminal

c) Übertragen des neuen Zählerstandes vom Terminal zur tragbaren Datenträgeranordnung

d) Schreiben des neuen Zählerstandes in den mittels des Ladesteuersignals (LAD) nur flüchtig aktivierten Wertbereich (WBA bzw. WBB) des nicht-flüchtigen Speichers (NVM)

e) nicht-flüchtig Aktivieren des Wertbereichs (WBB bzw. WBA) mit dem neuen Zählerstand durch Ändern des Zustands des Flagspeichers (FS).

10. Verfahren nach Anspruch 9, dadurch gekennzeichnet, daß nach dem Schritt d) folgende weiteren Schritte durchgeführt werden:

d1) Signieren des neuen Zählerstandes in der tragbaren Datenträgeranordnung und Übertragen der Signatur zum Terminal

d2) Ermitteln der Signatur des neuen Zählerstandes im Terminal und Vergleichen der beiden Signaturen,

daß der Schritt e) nur nach Übereinstimmung der beiden Signaturen durchgeführt wird und

daß bei Nicht-Übereinstimmung der beiden Signaturen das Verfahren abgebrochen wird.

11. Verfahren nach Anspruch 9 oder 10, dadurch gekennzeichnet, daß nach dem Schritt a) folgende weiteren Schritte durchgeführt werden:

a1) Lesen von für die tragbare Datenträgeranordnung spezifischen Daten aus der tragbaren Datenträgeranordnung mittels des Terminals

a2) Erzeugen einer Challenge und Ermitteln einer Response aus der Challenge und zumindest einem Teil der spezifischen Daten und dem alten Zählerstand im Terminal

a3) Übermitteln der Challenge und der Response vom Terminal zur tragbaren Datenträgeranordnung

a4) Ermitteln einer Response aus der Challenge in der tragbaren Datenträgeranordnung und Vergleichen der beiden Responses.

12. Verfahren nach Anspruch 9, 10 oder 11, dadurch gekennzeichnet, daß nach dem Schritt d) bzw. d2) folgende weiteren Schritte durchgeführt werden:

d3) Lesen von für die tragbare Datenträgeranordnung spezifischen Daten aus der tragbaren Datenträgeranordnung mittels des Terminals

d4) Erzeugen einer Challenge und Ermitteln einer Response aus der Challenge und zumindest einem Teil der spezifischen Daten und dem alten Zählerstand im Terminal

d5) Übermitteln der Challenge und der Response vom Terminal zur tragbaren Datenträgeranordnung

d6) Ermitteln einer Response aus der Challenge in der tragbaren Datenträgeranordnung und Vergleichen der beiden Responses

und daß nur bei Übereinstimmung der beiden Responses mit Schritt e) fortgefahren wird und bei Nicht-Übereinstimmung das Verfahren abgebrochen wird.

13. Verfahren nach einem der Ansprüche 10 bis 12, dadurch gekennzeichnet, daß zum Signieren eines Zählerstandes oder zum Erzeugen einer Response ein sich mit jedem Ladevorgang änderndes Datum verwendet wird und daß die Erzeugung einer Signatur oder einer Response mittels eines Pseude-Zufalls-Generators (PZG) erfolgt.

14. Verfahren nach Anspruch 13, dadurch gekennzeichnet, daß das Datum der Wert eines Ladezählers (LZ) ist, der jeden Ladevorgang zählt.

15. Verfahren nach Anspruch 13, dadurch gekennzeichnet, daß das Datum der Wert eines Signaturspeichers (SIGSP) ist, in den die Signatur des alten Werts des jeweils nicht-flüchtig aktiven Wertbereichs (WBA bzw. WBB) eingeschrieben wird.

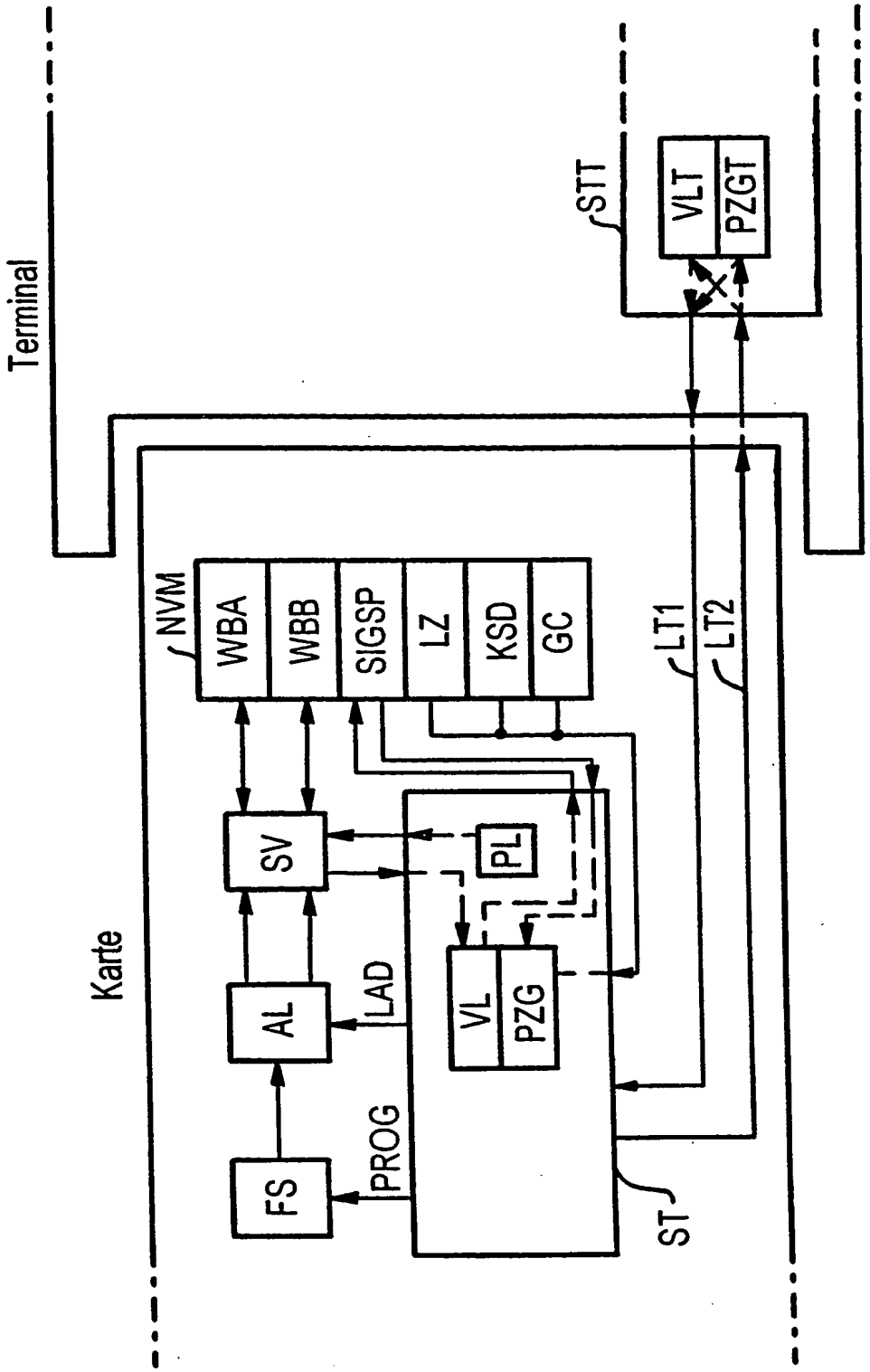
16. Verfahren nach Anspruch 13, dadurch gekennzeichnet, daß das Datum der Wert eines Signaturspeichers (SIGSP) ist, in den als Signatur des Ladevorgangs über das Ladeterminal bei jedem neuen Ladevorgang ein neuer Wert eingeschrieben wird.

17. Verfahren nach Anspruch 13, dadurch gekennzeichnet, daß vor jeder Responseberechnung ein Responsezähler (RZ) nicht-flüchtig geändert und als sich änderndes Datum verwendet wird.

Hierzu 1 Seite(n) Zeichnungen

– Leerseite –

Nummer: DE 44 39 266 A1
Int. Cl.: G 06 K 19/10
Offenlegungstag: 11. April 1996



602 015/439